

On Magic Finite Projective Space

David Nash and Jonathan Needleman

Abstract

This paper studies a generalization of magic squares to finite projective space $\mathbb{P}^n(q)$. We classify all functions from $\mathbb{P}^n(q)$ into a finite field where the sum along any r -flat is 0. In doing so we show connections to elementary number theory and the modular representation theory of $\mathrm{GL}(n, q)$.

Keywords: magic squares, finite projective space, incidence geometry, modular representation theory

1. Introduction.

This paper investigates a generalization of magic squares to finite projective space. A magic square can be viewed as an injective \mathbb{N} -valued function on a square grid where summing along any horizontal, vertical or main diagonal line will produce the same sum. Small [9] enlarged this definition of magic square by looking at k -valued functions on a square grid for some field k . He also removed the restriction that the functions be injective. In doing so, Small showed that the dimension of magic squares over a given field k is independent of k when $n \geq 5$ and depends on the characteristic of k for small n . The description of how the dimension is dependent on the characteristic is given in [6]. It is natural to extend Small's work to finite projective planes Π of order n , as the plane naturally comes with lines to sum over. In [8] we show that no non-constant functions $f : \Pi \rightarrow k$ exist unless the characteristic of k divides n .

This paper extends our previous work to finite projective space. For finite projective space we could require that all functions sum to the same value along each of the lines, however, there are other natural possibilities. For a field k and a k -valued function f on a finite projective space, we call f r -magic if it is injective and the sum of f over any r -dimensional subspace (r -flat) is a constant c independent of the r -flat. Such a c we call the magic sum. This definition is a little too restrictive because r -magic functions do not form an algebraic structure. Instead we weaken our definition to r -pseudomagic functions by removing the injectivity condition. These functions form a vector space and so will be easier to study. This differs from the terminology of Smith because we want to reserve magic functions to align with the historic term where magic objects have distinct values. We first will show for a projective space defined over a finite field \mathbb{F}_q , non-constant r -pseudomagic functions into a field k exist only if $\mathrm{char}(k) | q$. The remainder of the paper is dedicated to studying the

vector space of \mathbb{F}_q -valued, r -pseudomagic functions, for projective space defined over \mathbb{F}_q . We give a complete combinatorial classification all such functions as polynomials.

This problem can be viewed in terms of the 0-1 incidence matrix, A_r , of a projective space, which encodes the incidence structure of the points and r -flats in the projective space. Historically, when viewed over a characteristic p field, this matrix plays a crucial role in coding theory, and its p -rank has been studied extensively. For projective planes this rank is calculated by Goethals and Delsarte [3]. The result was generalized independently (and using different techniques) to the p -rank of the incidence matrix for points and hyperplanes in projective space by Graham and MacWilliams [4] and Smith [10]. Shortly thereafter Hamada generalized this further to the incidence matrix A_r [5]. This rank formula is now known as Hamada's formula. Despite all this work being completed in the late 1960s it is still an open question to determine the p -rank of general incidence matrices for r -flats and s -flats of projective space.

In 2000, Bardoe and Sin [1] used the modular representation theory of $\mathrm{GL}_n(q)$ in order to better understand, and reprove, Hamada's formula. In doing so they give a combinatorial description of the representation of $\mathrm{GL}_n(q)$ acting on functions over projective space. We use Bardoe and Sin's classification to study the r -pseudomagic functions, which happen to be closely related to $\mathrm{Ker} A_r$. This analysis helps give a geometric interpretation of Bardoe and Sin's combinatorial parameters of the representations.

2. Finite projective space and psuedomagic functions.

In this section we set notation and introduce finite projective space. Fix $q = p^t$ a prime power, \mathbb{F}_q a finite field of q elements, and K an algebraic completion of \mathbb{F}_q . We let $V(q)$ be an $n + 1$ dimensional vector space over \mathbb{F}_q with standard basis e_0, \dots, e_n , and let $V = V(q) \otimes K$ be an extension of $V(q)$ to an $n + 1$ dimensional vector space over K . We define $\mathbb{P}^n(q) = (\mathcal{L}_0, \dots, \mathcal{L}_{n-1})$ to be the projective space of dimension n defined over the field \mathbb{F}_q with \mathcal{L}_r the set of $r + 1$ -dimensional subspaces of $V(q)$ which we call r -flats. In the special case of $r = 0$ we call $\mathcal{P} = \mathcal{L}_0$ the points of $\mathbb{P}^n(q)$. Projective space $\mathbb{P}^n(q)$ comes equipped with an incidence relation. Subspaces $W_1, W_2 \subset V(q)$ are said to be incident, if $W_1 \subset W_2$ or $W_2 \subset W_1$, in this case we write $W_1 \sim W_2$.

Our interest was sparked by a desire to understand "labelings" of the points in $\mathbb{P}^n(q)$ which are magic for r -flats. That is, we are looking to understand functions $f : \mathcal{P} \rightarrow G$, for some Abelian group G , that satisfy two criteria:

- 1) There is a $c \in G$ so that for all $W_r \in \mathcal{L}_r$, $\sum_{p \sim W_r} f(p) = c$.
- 2) f is injective.

Functions satisfying both conditions we call r -magic, and those that satisfy condition 1) we call r -pseudomagic. In [8] we show that there are no non-trivial (non-constant) 1-pseudomagic functions for finite projective planes $\mathbb{P}^2(q)$ if G is a torsion-free group. We further show that there are no non-trivial 1-pseudomagic functions for $\mathbb{P}^2(q)$ unless G contains a cyclic group of order p . We

will let $r\text{-Mag}(\mathbb{P}^n(q), G) = \{f : \mathcal{P} \rightarrow G \mid f \text{ is } r\text{-pseudomagic}\}$. The functions where the magic sum is 0, are denoted by $r\text{-Mag}_0(\mathbb{P}^n(q), G)$.

The rest of this section is dedicated to showing that $r\text{-Mag}(\mathbb{P}^n(q), G)$ only contains constant functions, denoted by $\langle 1 \rangle$, if G does not contain a subgroup of order p . Note that we instead prove the equivalent statement that if G does not contain a subgroup of order p , then $r\text{-Mag}_0(\mathbb{P}^n(q), G) = \{0\}$. To prove this result we use two main ideas. First, we show the result is true for hyperplanes $((n-1)\text{-flats})$, and then we extend the result to arbitrary r -flats.

Lemma 1. *Let G be an Abelian group and let $n \geq 2$. If $(n-1)\text{-Mag}(\mathbb{P}^n(q), G) = \langle 1 \rangle$ then $(n-1)\text{-Mag}(\mathbb{P}^m(q), G) = \langle 1 \rangle$ for all $m \geq n$.*

Proof. Let $f \in (n-1)\text{-Mag}(\mathbb{P}^m(q), G)$. For any n -flat $W \subset \mathbb{P}^m(q)$, W is isomorphic to $\mathbb{P}^n(q)$, hence f restricted to W , $f|_W$, is the constant function g for some $g \in G$. Let $W_1, W_2 \subset \mathbb{P}^m(q)$ be n -flats. Let p_i be a point in W_i and let V be any n -flat containing p_1, p_2 . Then $f|_{W_1} = f|_V = f|_{W_2} = g$ for some $g \in G$. Since W_1, W_2 are arbitrary $f = g$. \square

Proposition 2. *If G has no subgroups of order p then $(n-1)\text{-Mag}(\mathbb{P}^n(q), G) = \langle 1 \rangle$ for all $n \geq 2$.*

Proof. We proceed by induction on n knowing that the statement is true when $n = 2$ by [8]. Assume $(r-1)\text{-Mag}(\mathbb{P}^r(q), G) = \langle 1 \rangle$. By Lemma 1 we have $(r-1)\text{-Mag}(\mathbb{P}^m(q), G) = \langle 1 \rangle$ for $m \geq r$. Let $V \in \mathbb{P}^{r+1}(q)$ be an $(r-1)$ -flat, and let

$$\mathcal{L}_r(V) = \{W \in \mathbb{P}^{r+1}(q) \mid W \text{ is an } r\text{-flat and } W \sim V\}$$

Note that $|\mathcal{L}_r(V)| = q + 1$ because through dualizing this is the same as the number of points on a line. Observe, for $f \in r\text{-Mag}(\mathbb{P}^{r+1}(q), G)$

$$\sum_{W \in \mathcal{L}_r(V)} f(W) = \sum_{p \notin V} f(p) + (q+1) \sum_{p \in V} f(p) = \sum_{p \in \mathbb{P}^{r+1}(q)} f(p) + q \sum_{p \in V} f(p)$$

Since f is r -pseudomagic and the sum is in terms of r -flats it is independent of V . Comparing to another $(r-1)$ -flat $V' \in \mathbb{P}^{r+1}(q)$ we have

$$q \sum_{p \in V} f(p) = q \sum_{p \in V'} f(p).$$

Since G contains no subgroup of order p the map $h \mapsto qh$ for $h \in G$ has a trivial kernel, and so we conclude $\sum_{p \in V} f(p)$ is independent of the choice of $(r-1)$ -flat V . That is, $f \in (r-1)\text{-Mag}(\mathbb{P}^{r+1}(q), G)$ and so f is a constant function. \square

Corollary 3. *If G has no subgroups of order p then $r\text{-Mag}_0(\mathbb{P}^n(q), G) = \{0\}$.*

Proof. This follows from Proposition 2 applied to Lemma 1. \square

Note that for a field K these results say that $r\text{-Mag}(\mathbb{P}^n(q), K) = \langle 1 \rangle$ if the characteristic of K does not divide q , so the interesting case is when the

characteristic of K and q are not relatively prime. The remainder of this paper we study $r\text{-Mag}(\mathbb{P}^n(q), \mathbb{F}_q)$ which for brevity we will just write as $r\text{-Mag}(\mathbb{P}^n(q))$. Similarly we let $r\text{-Mag}_0(\mathbb{P}^n(q), \mathbb{F}_q) = r\text{-Mag}_0(\mathbb{P}^n(q))$.

The incidence matrix of $\mathbb{P}^n(q)$ is closely related to $r\text{-Mag}_0(\mathbb{P}^n(q))$. Using the incidence relation we define a series of incidence matrices A_r for $0 < r < n$ as follows. The columns of A_r are indexed by the points \mathcal{P} and the rows are indexed by the r -flats \mathcal{L}_r . Then for $p \in \mathcal{P}$ and $W \in \mathcal{L}_r$ the (W, p) location is 1 if p and W are incident, and 0 otherwise. By viewing any function $f : \mathcal{P} \rightarrow \mathbb{F}_q$ as a column vector we may apply A_r as an operator on functions

$$A_r : \{f : \mathcal{L}_0 \rightarrow \mathbb{F}_q\} \longrightarrow \{g : \mathcal{L}_r \rightarrow \mathbb{F}_q\},$$

$$\text{where } (A_r \cdot f)(W) = \sum_{\substack{p \in \mathcal{L}_0 \\ p \sim W}} f(p).$$

This perspective brings about the insight that r -pseudomagic functions (with magic sum zero) correspond to the kernels of the incidence matrices A_r , i.e. $\text{Ker}(A_r) = r\text{-Mag}_0(\mathbb{P}^n(q))$.

3. Polynomials, Representation Theory, and Kummer's Binomial Theorem.

To study r -pseudomagic functions we first need to understand the functions $K[\mathbb{P}^n(q)] = \{f : \mathcal{P} \rightarrow K\}$. These can be characterized as polynomials in $n+1$ variables with certain restrictions. We choose coordinates X_0, \dots, X_n for V that are dual to the standard basis and look at which monomials $m \in K[X_0, \dots, X_n]$ restrict to functions on $\mathbb{P}^n(q)$. These monomials will then form a monomial basis for $K[\mathbb{P}^n(q)]$. For a monomial to be well-defined on points in projective space it must be invariant under scalar multiplication on the coordinates. By Fermat's little theorem this happens only when $q-1$ divides total degree of the monomial.

However, not all such monomials are unique when restricted to $\mathbb{P}^n(q)$. The kernel of the restriction map is generated by $\langle X_i^q - X_i \rangle_{i=0}^n$, along with δ_0 , the characteristic function of $0 \in V(q)$. The polynomials $X_i^q - X_i$ correspond to the fact that $c^q = c$ for all $c \in \mathbb{F}_q$, while δ_0 appears because projective space is defined for homogenous coordinates and is not defined at $0 \in V(q)$. To account for δ_0 in the kernel we set $X_0^{q-1} \dots X_n^{q-1} = 0$.

Before moving forward we introduce multi-index notation to help simplify the notation. Given a monomial $X_0^{b_0} \dots X_n^{b_n}$, denote the set of exponents by $\mathbf{b} = (b_0, \dots, b_n)$ and the monomial itself by $\mathbf{X}^{\mathbf{b}}$. The total degree of the monomial is then $|\mathbf{b}| = \sum_{i=0}^n b_i$. Using multi-index notation we summarize our discussion above by describing a monomial basis $\mathcal{M}(q)$ for $K[\mathbb{P}^n(q)]$.

$$\mathcal{M}(q) = \{\mathbf{X}^{\mathbf{b}} \mid 0 \leq b_i \leq q-1, (q-1) \nmid |\mathbf{b}|, \mathbf{b} \neq (q-1, \dots, q-1)\} \quad (1)$$

Our main goal is to determine which polynomials in $K[\mathbb{P}^n(q)]$ are r -pseudomagic. In order to do this we will make use of results from the representation theory of the group $\mathcal{G} = \text{GL}_{n+1}(q)$.

The group \mathcal{G} has a natural action on the vector space $V(q)$ which extends to an action on $\mathbb{P}^n(q)$. We use the action on $\mathbb{P}^n(q)$ to define an action of \mathcal{G} on $K[\mathbb{P}^n(q)]$ by setting $(g \cdot f)(x) = f(g^{-1}x)$ for all $g \in \mathcal{G}$, $f \in K[\mathbb{P}^n(q)]$, and $x \in \mathcal{P}$. Since the action of \mathcal{G} on $\mathbb{P}^n(q)$ sends r -flats to r -flats, it follows that $r\text{-Mag}_0(\mathbb{P}^n(q))$ (and hence $\text{Ker } A_r$) is a sub-representation. To gain information about the r -pseudomagic functions we study the structure of this representation.

To motivate the discussion we begin with a result from classical number theory.

Theorem 4 (Kummer's Theorem (1852)). *Let r be the largest natural number so that p^r divides $\binom{n}{k}$, then r is the number of carries involved in the base p sum of k and $n - k$.*

The original proof is due to Kummer [7]. We need a generalization of Kummer's Theorem to multinomial coefficients that is a result of Dickson [2].

Theorem 5. [2] *Let r be the largest natural number so that p^r divides the multinomial coefficient $\binom{k_1 + \dots + k_n}{k_1, \dots, k_n}$, then r is the sum of all the carries involved in the base p sum of $\sum_{i=1}^n k_i$.*

Understanding the representation generated by \mathcal{G} acting on X_0^{q-1} involves a special case of Theorem 5. For a generic $g \in \mathcal{G}$ that sends X_0 to $\sum_{i=0}^n a_i X_i$ we find that

$$g \cdot X_0^{q-1} = \sum_{b_0 + \dots + b_n = q-1} \binom{q-1}{b_0, \dots, b_n} (a_0^{b_0} \dots a_n^{b_n}) X_0^{b_0} \dots X_n^{b_n} \quad (2)$$

As we allow g to range over all of \mathcal{G} , the only monomials $\mathbf{X}^{\mathbf{b}}$ in (2) that appear in the generated space are precisely those where

$$p \nmid \binom{q-1}{b_0, \dots, b_n}$$

By Theorem 5 we can determine when p will divide the multinomial coefficient by analyzing the carries in the base p sum of $b_0 + \dots + b_n$. Hence, for any monomial $\mathbf{X}^{\mathbf{b}} \in K[\mathbb{P}^n(q)]$ we let $b_i = b_{i,0}p^0 + \dots + b_{i,t-1}p^{t-1}$ be the base p expansion of each b_i and recursively define r_{j+1} as the number so that

$$\sum_{i=0}^n b_{i,j} + r_j = (p-1) + r_{j+1}p, \quad (3)$$

where $r_0 = 0$. That is, r_j is exactly the number of carries into the p^j place of the base p sum $b_0 + \dots + b_n$. So for each monomial $\mathbf{X}^{\mathbf{b}} \in K[\mathbb{P}^n(q)]$ we can associate the list of carries (r_1, \dots, r_t) .

In our special case above, where $\mathbf{X}^{\mathbf{b}}$ is in the image of X_0^{q-1} under the action of \mathcal{G} , we have $|\mathbf{b}| = q-1$ and hence $r_t = 0$ as there is no carry into the p^t place. Now, by Theorem 5, the coefficient on $\mathbf{X}^{\mathbf{b}}$ is not divisible by p – and hence $\mathbf{X}^{\mathbf{b}}$ is in the representation generated by X_0^{q-1} – if and only if $(r_1, \dots, r_t) = (0, \dots, 0)$.

This example is also a special case of the representation theory of $\mathrm{GL}_{n+1}(q)$ acting on $K[\mathbb{P}^n(q)]$ developed by Bardoe and Sin in [1]. To each monomial $\mathbf{X}^{\mathbf{b}} \in K[\mathbb{P}^n(q)]$ we associate a sequence of t natural numbers $\mathbf{s} = (s_0, \dots, s_{t-1})$ in the set

$$\mathcal{H} = \{\mathbf{s} \mid 1 \leq s_i \leq n-1, ps_{i+1} - s_i \leq n(q-1), s_0 = \dots = s_{t-1} \neq n-1\}.$$

Let Fr_p be the Frobenius map which sends $a \in \mathbb{F}_q \mapsto a^p$. Let $\mathbf{X}^{\mathbf{b}} \in K[\mathbb{P}^n(q)]$. Since Fr_p is a field automorphism it acts on $K[\mathbb{P}^n(q)]$. Hence, $\mathrm{Fr}_p^{-i}(\mathbf{X}^{\mathbf{b}}) = \mathbf{X}^{\mathbf{b}'}$ in $K[\mathbb{P}^n(q)]$, and so $|\mathbf{b}'| = s_i(q-1)$ for some $s_i \in \mathbb{N}$ with $1 \leq s_i < n$. Then to $\mathbf{X}^{\mathbf{b}}$ we associate the sequence $\mathbf{s} = (s_i)_{i=0}^{t-1}$.

When $n \leq q-1$, \mathbf{s} can equivalently be defined as $s_i = r_i + 1$ for $1 \leq i \leq t-1$ and $s_0 = r_t + 1$ with r_i defined as in (3). So the set \mathcal{H} can be thought of as a parametrization of monomials in $K[\mathbb{P}^n(q)]$ which generalizes the data used in Kummer's theorem and its generalization.

The space \mathcal{H} also comes equipped with a partial order, $\mathbf{s} \leq \mathbf{s}'$ if $s_i \leq s'_i$ for all $0 \leq i \leq t-1$. This partial order allows one to define a “nice” collection of representations. Let

$$Y(\mathbf{s}) := \langle \text{all monomials associated to } \mathbf{s}' \leq \mathbf{s} \rangle$$

and let

$$\overline{Y}(\mathbf{s}) := \langle \text{all monomials associated to } \mathbf{s}' < \mathbf{s} \rangle$$

The following theorem is a compilation of the results from Bardoe and Sin which we will need.

Theorem 6. [1] *For each non-constant monomial $\mathbf{X}^{\mathbf{b}} \in K[\mathbb{P}^n(q)]$ there is an associated $\mathbf{s} \in \mathcal{H}$ and the following hold:*

1. $Y(\mathbf{s})$ and $\overline{Y}(\mathbf{s})$ are sub-representations of $K[\mathbb{P}^n(q)]$. Furthermore, $L(\mathbf{s}) := Y(\mathbf{s})/\overline{Y}(\mathbf{s})$ is irreducible.
2. The set $\{L(\mathbf{s}) \mid \mathbf{s} \in \mathcal{H}\}$ contains all irreducible representations that appear in the composition series of $K[\mathbb{P}^n(q)]/\langle 1 \rangle$.
3. The space generated by the action of \mathcal{G} on $\mathbf{X}^{\mathbf{b}}$ is $Y(\mathbf{s})$.

Returning to the example of \mathcal{G} acting on X_0^{q-1} we see that the \mathbf{s} associated to X_0^{q-1} is $\mathbf{s} = (1, \dots, 1)$. Since \mathbf{s} is the minimal element of \mathcal{H} , we know by Theorem 6 that

$$Y(\mathbf{s}) = \langle \mathbf{X}^{\mathbf{b}} \mid \text{The associated } \mathbf{s}' = (1, \dots, 1) \rangle.$$

This is the space generated by monomials where $r_0 = \dots = r_{t-1} = 0$, which is what we found using Theorem 5. In this light Theorem 6 can be thought of as a partial generalization of Kummer's Theorem, in that it describes when the coefficient of a monomial in the image $g \cdot \mathbf{X}^{\mathbf{b}}$, is not divisible by p in terms of base p expansions of \mathbf{b} . Specifically, if $\mathbf{X}^{\mathbf{b}} \in K[\mathbb{P}^n(q)]$ is acted on by $g \in \mathcal{G}$, then p does not divide the coefficient on a monomial $\mathbf{X}^{\mathbf{b}'}$ in the image if and only if $\mathbf{s}' \leq \mathbf{s}$, where $\mathbf{s}, \mathbf{s}' \in \mathcal{H}$ are associated to $\mathbf{X}^{\mathbf{b}}$ and $\mathbf{X}^{\mathbf{b}'}$ respectively. This result will allow us to describe which polynomials are in $r\text{-Mag}_0(\mathbb{P}^n(q))$ in terms of the parameters from \mathcal{H} .

4. Pseudomagic functions.

We now show which functions in $K[\mathbb{P}^n(q)]$ are r -pseudomagic.

Proposition 7. *For $0 < r < n$ if $m \in K[\mathbb{P}^n(q)]$, is a monomial of degree $r(q-1)$, then $m \in r\text{-Mag}_0(\mathbb{P}^n(q))$.*

Proof. Let $m = \mathbf{X}^{\mathbf{b}}$ where $|\mathbf{b}| = r(q-1)$. Instead of viewing m as a function on $\mathbb{P}^n(q)$ it will be easier to treat it as a function on $V(q)$, so we write \overline{m} for m viewed as function on $V(q)$. For $D \subset V(q)$ set $\overline{m}(D) = \sum_{d \in D} \overline{m}(d)$. Let $W \in \mathcal{L}_r$ be an r -flat of $\mathbb{P}^n(q)$ spanned by $\mathbf{x}_0, \dots, \mathbf{x}_r \in V(q)$ with coordinates $\mathbf{x}_i = [x_{i,0}, \dots, x_{i,n}]$ for each $0 \leq i \leq r$. Since all $\mathbf{X}^{\mathbf{b}} \in K[\mathbb{P}^n(q)]$ are constructed to be independent of the action of scalars, applying \overline{m} to a 1-flat $\langle \mathbf{x}_i \rangle$ gives

$$\begin{aligned} \overline{m}(\langle \mathbf{x}_i \rangle) &= \sum_{\alpha \in \mathbb{F}_q^*} \overline{m}(\alpha \mathbf{x}_i) = \sum_{\alpha \in \mathbb{F}_q^*} \overline{m}(\mathbf{x}_i) \\ &= -\overline{m}(\mathbf{x}_i) = -m(\mathbf{x}_i) \quad \text{for each } i. \end{aligned}$$

Since we want $m(W) = 0$ for all $W \in \mathcal{L}_r$, we just need to show $\overline{m}(W) = 0$.

$$\begin{aligned} \overline{m}(W) &= \sum_{(\alpha_0, \dots, \alpha_r) \in \mathbb{F}_q^{r+1}} \overline{m}(\alpha_0 \mathbf{x}_0 + \dots + \alpha_r \mathbf{x}_r) \\ &= \sum_{(\alpha_0, \dots, \alpha_r) \in \mathbb{F}_q^{r+1}} \left(\prod_{j=0}^n \left(\sum_{i=0}^r \alpha_i x_{i,j} \right)^{b_j} \right) \end{aligned} \quad (4)$$

Viewing (4) as a polynomial in $x_{i,j}$, the coefficient of $\prod_{j=0}^n \prod_{i=0}^r x_{i,j}^{a_{i,j}}$ is

$$\sum_{(\alpha_0, \dots, \alpha_r) \in \mathbb{F}_q^{r+1}} \left(\prod_{j=0}^n \binom{b_j}{a_{0,j}, \dots, a_{r,j}} \right) \prod_{i=0}^r \alpha_i^{(a_{i,0} + \dots + a_{i,n})}, \quad (5)$$

where $0 \leq a_{i,j} \leq b_j$ and $\sum_{i=0}^r a_{i,j} = b_j$ for all j .

We now show that each of these coefficients is zero. It is a well known fact that $\sum_{\alpha \in \mathbb{F}_q} \alpha^k = 0$ if and only if $(q-1) \nmid k$. Assume there is an i so that $(q-1)$ does not divide $A = \sum_{j=0}^n a_{i,j}$. Without loss of generality let $i = 0$, then the coefficient becomes

$$\sum_{(\alpha_1, \dots, \alpha_r) \in \mathbb{F}_q^r} C \left(\prod_{i=1}^r \alpha_i^{(a_{i,0} + \dots + a_{i,n})} \right) \left(\sum_{\alpha_0 \in \mathbb{F}_q} \alpha_0^A \right) = 0, \quad (6)$$

where

$$C = \left(\prod_{j=0}^n \binom{b_j}{a_{0,j}, \dots, a_{r,j}} \right).$$

Hence, we need only to consider the cases where $(q-1)$ divides $\sum_{j=0}^n a_{i,j}$ for all i . Since the total degree of our polynomial is equal to $r(q-1)$ it follows

there exists some i , $0 \leq i \leq r$ such that $\sum_{j=0}^n a_{i,j} = 0$. Suppose, without loss of generality, that $\sum_{j=0}^n a_{0,j} = 0$. Then our coefficient becomes

$$\sum_{\alpha_0 \in \mathbb{F}_q} \left(\sum_{(\alpha_1, \dots, \alpha_r) \in \mathbb{F}_q^r} \left(\prod_{j=0}^n \binom{b_j}{a_{0,j}, \dots, a_{r,j}} \right) \prod_{i=1}^r \alpha_i^{(a_{i,1} + a_{i,2} + \dots + a_{i,n})} \right).$$

The interior portion is constant with respect to the choice of α_0 , hence we are summing a constant q times, which gives 0 in \mathbb{F}_q . Since m is identically zero when summed over any r -flat W , it follows that $m \in r\text{-Mag}_0(\mathbb{P}^n(q))$ as desired. \square

Polynomials of degree $r(q-1)$ are not all the r -pseudomagic functions, but in some sense all of them are generated from these functions. The Frobenius map $\text{Fr}_p : x \mapsto x^p$ is a field automorphism, and thus composing it with any r -pseudomagic function will result in another r -pseudomagic function. By construction the Frobenius map cyclically permutes the sequence \mathbf{s} . For $m \in K[\mathbb{P}^n(q)]$ a monomial with degree $r(q-1)$ and associated sequence $\mathbf{s} \in \mathcal{H}$, we have by construction of \mathbf{s} that $s_0 = r$. Applying the Frobenius map to m will thus result in a monomial m' that has r in the associated sequence $\mathbf{s}' \in \mathcal{H}$. Furthermore, if $m \in r\text{-Mag}_0(\mathbb{P}^n(q))$, then $m \in r'\text{-Mag}_0(\mathbb{P}^n(q))$ for all $r < r' < n$ as well. This follows because each point in a fixed r' -flat W will be incident to exactly ℓ r -flats in W , where $\ell \equiv 1 \pmod{p}$. So summing over all r -flats within a given r' -flat is the same as summing over the r' -flat. We can sum up our discussion with the following corollary:

Corollary 8. *If $m \in K[\mathbb{P}^n(q)]$ is a monomial associated to $\mathbf{s} \in \mathcal{H}$ and there is an i so that $s_i \leq r$, then $m \in r\text{-Mag}_0(\mathbb{P}^n(q))$.*

To finish we show the condition in Corollary 8 is sufficient. That is, if $m \in K[\mathbb{P}^n(q)]$ is a monomial associated to $\mathbf{s} \in \mathcal{H}$ and $s_i > r$ for all $0 \leq i \leq t-1$ then $m \notin r\text{-Mag}_0(\mathbb{P}^n(q))$.

We analyze the monomial $m_r = X_0^{q-1} \dots X_r^{q-1}$ which is associated to $(r+1, \dots, r+1) \in \mathcal{H}$. Consider the r -flat $W \subset V(q)$ generated by e_0, \dots, e_r . For $v = \alpha_0 e_0 + \dots + \alpha_r e_r \in W$ with $\alpha_i \in \mathbb{F}_q$ we have

$$m_r(v) = \begin{cases} 0 & \text{if } \alpha_j = 0 \text{ for some } j \\ 1 & \text{else} \end{cases}$$

and so we have

$$m_r(W) = - \sum_{(\alpha_0, \dots, \alpha_r) \in (\mathbb{F}_q^*)^{r+1}} 1 = -|(\mathbb{F}_q^*)^{r+1}| = -(q-1)^{r+1} \neq 0 \in \mathbb{F}_q$$

Hence $m_r \notin r\text{-Mag}_0(\mathbb{P}^n(q))$. However, it is not in $r\text{-Mag}(\mathbb{P}^n(q))$ either, since m_r is zero on every point in the r -flat W' generated by e_1, \dots, e_{r+1} since the coefficient of e_0 is always 0 for $v \in W'$.

Now let $\mathbf{s} \in \mathcal{H}$ with $s_i > r$ for all i , and let m be a monomial associated to \mathbf{s} . If we assume that $m \in r\text{-Mag}_0(\mathbb{P}^n(q))$ then by Theorem 6, $Y(\mathbf{s}) \subset r\text{-Mag}_0(\mathbb{P}^n(q))$. This implies that $Y(r+1, \dots, r+1) \subset Y(\mathbf{s}) \subset r\text{-Mag}_0(\mathbb{P}^n(q))$ and hence $m_r \in r\text{-Mag}_0(\mathbb{P}^n(q))$, which we just showed to be false. Summarizing our discussion we have our main theorem characterizing $r\text{-Mag}_0(\mathbb{P}^n(q))$.

Theorem 9. *If $m \in K[\mathbb{P}^n(q)]$ is a monomial associated to $\mathbf{s} \in \mathcal{H}$, then $m \in r\text{-Mag}_0(\mathbb{P}^n(q))$ if and only if $\min\{s_0, \dots, s_n\} \leq r$.*

5. Conclusions and further questions.

Theorem 9 helps give a geometric interpretation to the combinatorial set \mathcal{H} . The minimum of the terms in $\mathbf{s} \in \mathcal{H}$ gives geometric information about the functions $f \in Y(\mathbf{s})$. Since $K[\mathbb{P}^n(q)]$ is a geometric object we expect there is a way to geometrically distinguish representations $Y(\mathbf{s})$ and $Y(\mathbf{s}')$ when \mathbf{s} and \mathbf{s}' have the same minimum.

We would also like to see a deeper connection of the set \mathcal{H} to a generalization Kummer's theorem. As of now we can only use \mathcal{H} to describe when a prime p divides a coefficient of a term in the image of a monomial under the action of \mathcal{G} . Given that the data \mathcal{H} provides is closely related to what is needed for Kummer's theorem we expect that one can expand on Theorem 6 to determine the exact power of p dividing a coefficient of a term in the image of a monomial under the action of \mathcal{G} .

Finally, our original goal was to find functions which are r -magic for projective space (injective r -pseudomagic functions). We know there are no r -magic functions into \mathbb{F}_q since $|\mathbb{P}^n(q)| = (q^{n+1} - 1)/(q - 1)$, but there is a chance that such a function exists mapping into \mathbb{F}_q^n . That is, it is theoretically possible for $[r\text{-Mag}_0(\mathbb{P}^n(q))]^n$ to contain an injective function. It is our hope that our main result, Theorem 9, which characterizes $r\text{-Mag}_0(\mathbb{P}^n(q))$ in terms of polynomials will help lead to a concrete construction of such a function.

References

- [1] M. Bardoe, P. Sin, The permutation modules for $\text{GL}(n+1, \mathbf{F}_q)$ acting on $\mathbf{P}^n(\mathbf{F}_q)$ and \mathbf{F}_q^{n-1} , J. London Math. Soc. (2) 61 (1) (2000) 58–80.
URL <http://dx.doi.org/10.1112/S002461079900839X>
- [2] L. E. Dickson, Theorems on the residues of multinomial coefficients with respect to a prime modulus, Quart. J. Pure Appl. Math. 33 (1902) 378–384, jFM:33.0203.02.
- [3] J.-M. Goethals, P. Delsarte, On a class of majority-logic decodable cyclic codes, IEEE Trans. Information Theory IT-14 (1968) 182–188.
- [4] R. L. Graham, J. MacWilliams, On the number of information symbols in difference-set cyclic codes, Bell System Tech. J. 45 (1966) 1057–1070.

- [5] N. Hamada, The rank of the incidence matrix of points and d -flats in finite geometries, J. Sci. Hiroshima Univ. Ser. A-I Math. 32 (1968) 381–396.
- [6] X.-d. Hou, A. G. Lecuona, G. L. Mullen, J. A. Sellers, On the dimension of the space of magic squares over a field, Linear Algebra Appl. 438 (8) (2013) 3463–3475.
URL <http://dx.doi.org/10.1016/j.laa.2012.12.014>
- [7] E. E. Kummer, Über die ergänzungssätze zu den allgemeinen reciprocitätsgesetzen, J. für die reine und angewandte Math. 44 (1852) 93–146.
URL <http://eudml.org/doc/147500>
- [8] D. Nash, J. Needleman, When are finite projective planes magic?, preprint.
- [9] C. Small, Magic squares over fields, Amer. Math. Monthly 95 (7) (1988) 621–625.
URL <http://dx.doi.org/10.2307/2323304>
- [10] K. J. C. Smith, On the p -rank of the incidence matrix of points and hyperplanes in a finite projective geometry, J. Combinatorial Theory 7 (1969) 122–129.